

A

UTILITY PATENT APPLICATION TRANSMITTAL

(Small Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
2308/102Total Pages in this Submission
39**TO THE ASSISTANT COMMISSIONER FOR PATENTS**Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

APPARATUS AND METHOD FOR AUTHENTICATED MULTI-USER PERSONAL
INFORMATION DATABASE

and invented by:

Bruce D. Sunstein
Eileen C. ShapiroIf a **CONTINUATION APPLICATION**, check appropriate box and supply the requisite information:☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Enclosed are:

Application Elements

1. ☐ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 25 pages and including the following:
 - a. ☒ Descriptive Title of the Invention
 - b. ☒ Cross References to Related Applications (if applicable)
 - c. ☐ Statement Regarding Federally-sponsored Research/Development (if applicable)
 - d. ☐ Reference to Microfiche Appendix (if applicable)
 - e. ☒ Background of the Invention
 - f. ☒ Brief Summary of the Invention
 - g. ☒ Brief Description of the Drawings (if drawings filed)
 - h. ☒ Detailed Description
 - i. ☒ Claim(s) as Classified Below
 - j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL
(Small Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
2308/102

Total Pages in this Submission
39

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
a. ☐ Formal b. ☒ Informal Number of Sheets 6
4. ☒ Oath or Declaration
a. ☐ Newly executed *(original or copy)* ☒ Unexecuted
b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
c. ☒ With Power of Attorney ☐ Without Power of Attorney
d. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application,
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Computer Program in Microfiche
7. ☐ Genetic Sequence Submission *(if applicable, all must be included)*
a. ☐ Paper Copy
b. ☐ Computer Readable Copy
c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☐ Assignment Papers *(cover sheet & documents)*
9. ☐ 37 CFR 3.73(b) Statement *(when there is an assignee)*
10. ☐ English Translation Document *(if applicable)*
11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☒ Certificate of Mailing
☐ First Class ☒ Express Mail *(Specify Label No.):* EL361 718 178US

UTILITY PATENT APPLICATION TRANSMITTAL
(Small Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
2308/102

Total Pages in this Submission

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☐ Small Entity Statement(s) - Specify Number of Statements Submitted: _____
17. ☐ Additional Enclosures (please identify below):

Fee Calculation and Transmittal


CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	39	- 20 =	19	x \$9.00	\$171.00
Indep. Claims	5	- 3 =	2	x \$39.00	\$78.00
Multiple Dependent Claims (check if applicable) <input checked="" type="checkbox"/>					\$130.00
BASIC FEE					\$380.00
OTHER FEE (specify purpose) _____					\$0.00
TOTAL FILING FEE					\$759.00

- ☐ A check in the amount of _____ to cover the filing fee is enclosed.
- ☐ The Commissioner is hereby authorized to charge and credit Deposit Account No. _____ as described below. A duplicate copy of this sheet is enclosed.
- ☐ Charge the amount of _____ as filing fee.
 - ☐ Credit any overpayment.
 - ☐ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
 - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated: November 24, 1999

Signature


Bruce D. Sunstein
Reg. No. 27,234
BROMBERG & SUNSTEIN LLP
125 Summer Street
Boston, Massachusetts 02110-1618
(617) 443-9292
(617) 443-0004 FAX

cc:

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)

Applicant(s): Sunstein et al.

Docket No.

2308/102

Serial No.
unassignedFiling Date
filed herewithExaminer
unassignedGroup Art Unit
unassignedInvention: **APPARATUS AND METHOD FOR AUTHENTICATED MULTI-USER PERSONAL
INFORMATION DATABASE**I hereby certify that this utility patent application and enclosures referred to herein
(Identify type of correspondence)is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under
37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on
November 24, 1999
(Date)Bruce D. Sunstein

(Typed or Printed Name of Person Mailing Correspondence)

A handwritten signature in dark ink, appearing to read "B. Sunstein", written over a horizontal line.

(Signature of Person Mailing Correspondence)

EL361 718 178US

("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application for

**Apparatus and Method for Authenticated Multi-User
Personal Information Database**

Invention of: Bruce D. Sunstein
 Eileen C. Shapiro

Attorney docket number:
2308/102

Attorneys:
Bromberg & Sunstein LLP
125 Summer Street
Boston, MA 02110-1618
Tel: (617) 443-9292
Fax: (617) 443-0004

**Apparatus and Method for Authenticated Multi-User
Personal Information Database**

The present application claims priority from provisional application serial
5 number 60/125,234, filed March 19, 1999, for an invention of the same inventors
and title as herein; such application is hereby incorporated herein by reference.

Technical Field

The present invention relates to personal information and medical
databases, and particularly to databases used in connection with financial
10 transactions and medical emergencies.

Background Art

With the rise of digital communications for a wide range of applications, it
is now a commonplace for important financial transactions, and even everyday
transactions, to occur over networks of all kinds, including local area networks
15 (LANs and intranets), wide area networks (WANs and extranets), and the
Internet. Formerly these transactions were in many cases conducted in person or
over the telephone under circumstances where it was often relatively easy for
each person to be assured that the other party is actually the person who the
party purports to be — namely, to be assured that the party is authentic.
20 Moreover, such transactions commonly occurred under conditions where the
universe of potential parties was relatively limited. Authenticity could under
those circumstances often be determined by visual inspection (when the
transaction is in person) or by personal recognition of a voice (when the
transaction is over the telephone).

25 When the transactions are conducted over a network, identifying
information associated with in-person or telephone-based transactions is far more
difficult to obtain. Moreover, the universe of potential parties to such
transactions is significantly expanded. These circumstances provide an
opportunity for individuals to misappropriate in whole or in part the identity of
30 another person for personal gain or other improper purposes. A partial
misappropriation of identity occurs in the case of credit card fraud. In addition

there are increasing instances of wholesale identity theft, where the perpetrator assumes the identity of another for a continuing series of fraudulent transactions. Indeed, even in-person and telephone-based transactions provide opportunities for identity theft.

- 5 In addition, the ubiquitous nature of the Internet has had an effect on information, essentially personal in nature, which has formerly inhabited the domain of private individuals and their immediate communities, and made that information available to the public; the Internet allows much private information to be transformed into public information. Associated with this loss of privacy is
- 10 in general a greater risk of identity theft.

- Central credit card registries exist to provide credit card owners with a single point of reference for registering credit card numbers and, optionally, providing selected other services for dealing with lost or stolen credit cards (e.g., notifying credit card issuers of the theft). However, a credit card registry may
- 15 itself be used by an unscrupulous individual to perpetrate an identity theft, whereby, for example, a fraudulent change of address may be given to multiple credit card issuers via a credit card registry.

- Smart cards typically include data pertaining to the card holder, but in many instances, smart cards will not protect against identity theft; indeed, even
- 20 with enhanced security, it may be assumed that smart thieves will or could find ways to steal smart cards and that the information stored on these cards may also be stolen.

- In another context, authentication-related issues may be important when a person may have critical information to impart but is unexpectedly impaired (for
- 25 example by reason of an accident or a stroke while traveling alone, etc.). The impaired person, for example, may have certain strictures governing medical treatment (for example, allergy to penicillin) or important preferences as to the scope of medical treatment to be rendered under life-threatening conditions and as to persons to be involved in deciding about such treatment.

- 30 Summary of the Invention

In a first embodiment, the invention provides a method of assuring

integrity of a personal information data base containing personal information provided by multiple users. The method includes:

- a. obtaining a user's personal information from the user;
- b. obtaining a first set of physiological identifiers associated
5 with the user;
- c. storing, in a digital storage medium, a data set pertinent to the user, the data set including the user's personal information and a representation of the physiological identifiers associated with the user;
- d. permitting a subject to modify information in the stored data
10 set pertinent to the user only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as the user.
- 15 What this embodiment may achieve in some aspects is a circumstance wherein individual identity may be established by a user in a proprietary database and wherein that identity is safeguarded. In this manner the user is put in control of the content relating to his identity, but parameters relevant to that identity may be changed only under conditions wherein the risk of identity theft is reduced.
- 20 In a further embodiment, the method includes obtaining a user's medical information from the user, and the data set includes the user's medical information.

Definitions. As used in this description and the accompanying claims, the following terms shall have the meanings indicated, unless the context otherwise
25 requires:

- (i) A user's "personal information" includes (a) any alphanumeric identifier of a particular natural person used or issued by a governmental authority or a merchant in connection with the user, such as a credit card number of the user, the user's passport number, the user's social security number, the user's tax
30 identification number, driver's licence number, checking account numbers, etc., together with the identity of the governmental authority, banking or financial

institution in each case; (b) the user's name; and (c) contact information pertinent to the user. Optionally, "personal information" may include any or all of the following: (i) any variant of the user's name used by such governmental authority or merchant and (ii) the particular contact information used by such

5 governmental authority or merchant for communicating with the user.

(ii) A "merchant" includes any banking or financial institution or any person or entity (including a retail establishment, hospital, or educational institution) providing services or goods for monetary consideration.

(iii) "Contact information" pertinent to a natural person includes
10 information pertinent to communicating with the person, such as the person's home or business address or telephone number or E-Mail address.

(iv) A user's "medical information" includes (a) the name of a natural person, in a caring relation to the user, whom the user wishes to be notified in the event of the user's illness, injury, or death and (b) contact information pertinent
15 to the caring natural person. Optionally, "medical information" may include any or all of the following: (i) medical treatment information, including medical conditions (such as allergy to penicillin) and religious requirements (for example barring blood transfusions), important to treating the user under emergency circumstances; (ii) information concerning participation by the user in any organ
20 donor program; (iii) health proxy and living will information, concerning scope of medical treatment desired by the user under severe medical circumstances; (iv) the name of any person holding a health proxy of the user and contact information pertinent to such person; and (v) health provider and health insurance information pertinent to the user.

(v) A "physiological identifier associated with a user" is physiological
25 feature of the user, capable of uniquely identifying the user, such as, for example, the appearance of the user's face, a fingerprint of the user, the configuration of an iris in an eye of the user, the user's voice or speech (that is, characteristics of utterances of the user), a sample of the user's DNA, or the sequence of a relevant
30 portion of such a DNA sample.

(vi) A "representation" of a physiological identifier is an abstraction,

capable of being stored in a digital storage medium, of the physiological identifier, that retains characteristics of the identifier to a degree sufficient to permit reasonably reliable discrimination between the user and another natural person. The abstraction may, for example, be a digitized photograph of the user's face, and the photograph may be manually or automatically compared with the face of a subject purporting to be the user.

(vii) The term "set" is used in the mathematical sense, and a "set" is not empty; that is, a "set" has at least one member.

(viii) A "multiplicity" of terminals means at least three terminals.

(ix) A "physiological identifier transducer" includes any device (such as a fingerprint reader or a voice terminal/analyzer) that transforms physical information, derived from a physiological feature of a human subject that is capable of uniquely identifying the subject, into computer-readable data useful for identifying the subject.

(x) An account that "authorizes the transfer of funds" is one such as a checking account, a debit card account, or a credit card account.

(xi) An account that is "based on the extension of credit to the account holder" includes a wide variety of account relationships, including those based on the furnishing of goods or services wherein the cost of the goods or services is billed to the recipient or to a third party after the account is opened. Examples include health care services billed to an insurer, stock brokerage margin accounts, etc.

In a series of further and important embodiments, the first set of physiological identifiers may include a plurality of members. In this way, the level of reliability in determination of authenticity may be selected in accordance with requirements of existing circumstances. For example, embodiments of the invention include methods and systems wherein the first set of identifiers includes at least one member selected from the group consisting of a fingerprint of the user and the configuration of an iris in an eye of the user and at least one member selected from the group consisting of characteristics of utterances of the user and the appearance of the user's face. These two groups offer differing levels

of reliability— fingerprints and iris configuration offering potentially greater reliability than characteristics of utterances of the user and the appearance of the user's face, since both utterances and facial appearance can be disguised. On the other hand, it may be more convenient to utilize characteristics of utterances or facial appearance for authentication. In circumstances where such convenience outweighs the risks associated with the reduced level of reliability, these forms of authentication may be used, even though more reliable forms of authentication might be required, for example, for user modification of data in the user's data set.

10 A related embodiment of a system in accordance with the present invention provides a multiplicity of remotely distributed terminals in communication with the data base, and each terminal includes a physiological identifier transducer and a communication link to a merchant. (The communication link may be as simple as a telephone connection, or it may be a data network directly to the merchant or indirectly over a path that includes the data base, or it may be over the Internet.) In this fashion, a user may, for example, enter into a transaction with the merchant over the Internet or over the telephone, and then physically go to a location near the user where a terminal is located, and use the terminal to authenticate the transaction. Or the transaction may be entered into at the terminal at substantially the same time as it is authenticated. Transactions wherein this system may be used include, for example, those over a desired threshold amount. This system therefore includes a multi-user personal information data base, a multiplicity of remotely distributed terminals in communication with the data base and having a communication link with a merchant, and an authenticity checker which determines whether there is a sufficient match between the output of a physiological identifier transducer attributable to a subject purporting to be a user and a physiological identifier in the first. The data base includes, for each user, a data set pertinent to such user, and the data set including such user's personal information obtained from the user and a representation of a first set of physiological identifiers associated with the user.

In a further embodiment of methods and systems in accordance with the present invention, a subject is permitted to modify information in the stored data set only if the subject provides the new set of physiological identifiers under a condition permitting verification, independent of the physiological identifiers, that the new set is being provided by the person purporting to provide them. Such a condition may include the physical presence of the subject when providing the new set. Alternatively, or in addition, the condition may include having the subject provide the new set when prompted to do so or having the subject provide a non-physiological identifier. The non-physiological identifier may be selected from the group consisting of a password and a pass card. Alternatively, the non-physiological identifier is provided in the course of a session, over a computer network, employing a user's public and private keys.

In yet another related embodiment, there is provided a method for authenticating a user transaction. The method includes obtaining a test set of physiological identifiers from a subject purporting to be the user and accessing information in the data set pertinent to the user stored in accordance with embodiments previously described. The method also includes determining if there is a sufficient match between at least one member in the test set and a corresponding physiological identifier represented in the data set. In a further related embodiment, the database is accessible via a server at a first location; obtaining the test of physiological identifiers is performed at a second location remote from the first location; and determining if there is a sufficient match includes communicating with the server from the second location over a network. The network may, for example, be a global communication network, such as the Internet. Optionally, obtaining the test set of physiological identifiers is performed under supervision of a merchant. As an additional option, determining if there is a sufficient match may be performed without revealing content of the first data set to the merchant. Indeed, the entire data base may be maintained in a manner that it is confidential to the merchant.

In further related embodiments, the transaction is a change of address for an account. In another embodiment, the transaction is an application to open an

account. In either of these embodiments, the account may be one that authorizes the transfer of funds. Alternatively, or in addition, the account may be based on the extension of credit to the account holder.

5 In another further related embodiment, the transaction is an application to a government agency for one of a license and a renewal of a license. The license may be, for example, a driver's license or a passport, or a professional license. Alternatively, the transaction is an application to a government agency for one of an identification token and a renewal of an identification token. The identification token, for example, may be an identification card or a social security number.

10 In another embodiment, the invention provides a digital storage medium on which has been recorded a multi-user personal information data base. The data base includes, for each user, a data set pertinent to such user. This data set includes:

- (a) such user's personal information obtained from the user;
- 15 (b) an authentication set of physiological identifiers associated with the user; and
- (c) such user's emergency information obtained from the user.

In yet another embodiment the invention provides a system for updating a personal information database containing a data set for each one of multiple
20 users. Each data set including a user's personal information and a representation of a first set of physiological identifiers associated with the user. The system of this embodiment includes:

- a physiological identifier transducer having an output representing a physiological identifier associated with a subject;
- 25 a user access authorization module, coupled to the physiological identifier transducer, the database, for determining whether the output of the physiological identifier transducer sufficiently matches the representation of the first set of physiological identifiers, so that the subject is authenticated as the user;
- 30 a user data set access module, coupled to the user access authorization module and to the database, for accessing the user data set, in the event that the

only on a selected basis to authorized parties and in accordance the appropriate context. Finally, the registration system in accordance with this embodiment may be managed in cooperation with law enforcement agencies to deter fraudulent use by providing physiological identifiers in the form, for example, of

- 5 photographs and fingerprints, when probable cause has been established for disclosure to law enforcement agencies, as evidenced by the issuance of a search warrant.

An information registry that is consistently managed in accordance with the embodiment described in the previous paragraph may be expected to become
10 a trusted source of the information which it stores. updated contact information.

We have referred above to a "physiological identifier associated with a user" as a physiological characteristic of the user, capable of uniquely identifying the user. We gave as examples, the appearance of the user's face, a fingerprint of the user, the configuration of an iris in an eye of the user, characteristics of the
15 user's voice or speech (i.e, characteristics of utterances of the user), a sample of the user's DNA, or the sequence of a relevant portion of such a DNA sample. Further information about the technology associated with the use of physiological identifiers of this nature in a computing environment appears in an article by G. Gunnerson, "Are you ready for Biometrics?", 18 *PC Magazine*, No. 4,
20 160-178 (February 23, 1999). This article, which is incorporated herein by reference in its entirety, discloses commercially available products to protect against unauthorized computer system access by utilization of a physiological identifier such as fingerprint, facial appearance, and characteristics of one's voice and speech, sometimes in tandem with a non-physiological identifier such as a
25 smart card or a password. See also the content, which is hereby incorporated herein by reference in its entirety, of the following web sites: www.biometrics.org (The Biometric Consortium), www.emory.edu/BUSINESS/et/biometric/ (biometric technology explained at Emory University site), <http://webusers.anet-stl.com/~wrogers/biometrics/> (The Biometric Digest).

- 30 In Fig. 1 is shown a block diagram of a preferred embodiment of a method in accordance with the present invention. This embodiment includes two phases,

an enrollment phase 111 and a modification phase 112. In the enrollment phase, personal information is obtained from the user in box 11. Optionally medical information is also obtained from the user. Next in box 12 there is obtained a first set of physiological identifiers associated with the user. In box 13 the user data set, which includes the user's personal information (and optionally medical information obtained from the user) and a representation of the physiological identifiers associated with the user, is stored in the database.

In the modification phase 112, a subject is permitted to modify data in the user's data set if it is determined that the subject is the user. In box 14, there is received a new set of physiological identifiers from the subject. In box 15, there is conducted a test to determine whether there is a sufficient match between the new set of physiological identifiers and the first set of physiological identifiers obtained in box 12. If the match is not sufficient, then in box 17 it is prohibited to modify the data set. Alternatively, if the match is sufficient, then, in box 16, the subject (who is authenticated as the user) is permitted to modify the data set.

Once the enrollment phase 111 is complete, so that a first set of physiological identifiers has been obtained from the user, it is possible to use the enrolled information to authenticate a transaction in a manner generally analogous to the modification phase 112 discussed above in connection with Fig. 1. Fig. 2 thus presents a block diagram of an embodiment of the invention employed for authentication of a transaction in a manner analogous to the modification phase 112 of Fig. 1. Thus in box 24 there is received a test set of physiological identifiers from the subject. In box 25, there is conducted a test to determine whether there is a sufficient match between the test set of physiological identifiers and the first set of physiological identifiers obtained in box 12. If the match is not sufficient, then in box 27 it is prohibited to modify the data set. Alternatively, if the match is sufficient, then, in box 26, the subject (who is authenticated as the user) is permitted to modify the data set.

In Fig. 3 is illustrated in schematic form a structure for a database in accordance with an embodiment of the present invention. Row 311 illustrates a record for user 1. A first portion 31 of the record is used to store user 1 personal

information. Another portion 32 of the record is used to store a set of physiological identifiers associated with user 1. Another portion 33 of the record is used to store emergency information pertinent to user 1. A similar structure is employed for each other user, illustrated in row 341 for user n , so that a first

5 portion 34 of the record stores user n personal information, a second portion 35 stores user n set of physiological identifiers, and a third portion 36 stores user n emergency information. Although the structure of the database illustrated here provides a contiguous record for each user, it is within the scope of the present invention to provide a database where the information associated with a given

10 user is stored in a manner that the information associated with a given user is not contiguous. For example, the information for a given user may be stored in various elements in various locations and accessed by an index that is common to all elements for any given user. A wide range of data structures may be implemented in accordance with procedures known in the art.

15 In Fig. 4 is shown a block diagram of an embodiment of the present invention providing a system for updating a personal information database 41 containing a data set for each one of multiple users. Each data set, as described in connection with Fig. 3, includes a user's personal information and a representation of a first set of physiological identifiers associated with the user.

20 The system of this embodiment includes a physiological identifier transducer 42 having an output representing a physiological identifier associated with a subject. A user access authorization module 43, triggered by user input 46, is coupled to the physiological identifier transducer 42 and also to the database 41. This module obtains from the database 41 the representation of the first set of

25 physiological identifiers associated with the user who the subject purports to be. The representation data is compared with the output of the physiological identifier transducer 42 to determine whether there is a sufficient match between the first set of physiological identifiers and the physiological identifier data produced by the transducer 42. When the match is sufficient, the subject is

30 authenticated as the user.

The output of the user access authorization module 43 is provided to the

user data set access module 44. The user data set access module 44 is coupled to the user access authorization module 43 and to the database 41. In the event that the user access authorization module 43 has authenticated the subject as the user, the user data set access module 44 accesses the user data set in the database 41.

- 5 The user data set update module 45 is coupled to the user data set access module 44, as well as to the database 41 and to the user input 46; the user data set update module 45 then permits the user to update such user's corresponding data set in the database.

- Fig. 5 illustrates operation of the user access authorization module 43 of Fig. 4. This module in fact includes three components. The first component is the physiological identifier data set fetch 51. This component obtains representation data from the database 41 pertaining to the first set of physiological identifiers associated with in the user who the subject purports to be. The component 51 passes the data fetched to the physiological identifier data set comparator 52, which compares the fetched data with the data from the physiological identifier transducer 42. The authorization processor 53 takes the output of the comparator 52 and provides an authorization signal to the user data set access module 44 in the event of a sufficient match found by the comparator 52.

- Fig. 6 is a block diagram of an embodiment of a system in accordance with the present invention providing a multiplicity of remotely distributed terminals in communication with a multi-user personal information data base. The multi-user database, item 61, is a database of the general type described above in connection with Figs. 1 through 4. The database includes a data set pertinent to each user. Each data set includes a first set of physiological identifiers associated with the user. Each data set also includes such user's personal information obtained from the user, and optionally such user's medical information. A multiplicity of remotely distributed terminals, shown here as items 66, 67, and 68, are in communication with the database 61 over one or more networks. For example, the terminals 66-68 may be in communication with the database 61 over the Internet. Each of these terminals may include similar components, and for convenience we discuss the components of terminal 66. The terminal of this

embodiment includes a fingerprint reader 62 and a voice terminal/analyzer 63. Each of the items 62 and 63 is, more broadly stated, a physiological identifier transducer, namely a device that transforms physical information, derived from a physiological feature of a human subject that is capable of uniquely identifying the subject, into computer-readable data useful for identifying the subject. (Alternatively or additionally, the physiological identifier transducer may be employed). Thus a user may utilize the fingerprint reader 62 and the voice terminal/analyzer 63 to provide a set of physiological identifiers that are represented and stored as part of such user's data set in the general manner described above in connection with Fig. 1.

Alternatively, or in addition, the user may wish to authenticate a transaction being made with a merchant. In this connection, the user may utilize either the fingerprint reader 62 or the voice terminal/analyzer 63, or both of them, from which may be derived a test set of physiological identifiers in a manner described previously in connection with Fig. 2. The authenticity checker 65 is then used to retrieve physiological identifier data stored as part of the user's data set in the database 61 and then to determine whether data from the test set of physiological identifiers sufficiently matches the corresponding retrieved data. The results of the match determination are then communicated with the merchant using the communication link 64.

Although the authenticity checker 65 is shown in Fig. 6 as part of the terminal 66, it may in fact be located remotely from the terminal over a suitable network, and may be conveniently located at the same network node, for example, as the database 61. In such a case, the physiological identifier transducer data from the fingerprint reader 62 and the voice terminal/analyzer 63 may be transmitted over the network to the remotely located authenticity checker for determination of the sufficiency of the match with the corresponding retrieved data. Similarly, the communication link 64 may optionally run from a location other than the terminal to the merchant; for example, where the checker is physically adjacent to the database 61, the link 64 may run from the checker to the merchant. In a simple embodiment, the authenticity checker 65 is part of the

terminal 66 and includes a display for readout by a human operator; and the link 64 is a manually operable telephone providing a dial-up telephone connection to the merchant. In this manner, a human operator may supervise operation of the physiological identifier transducers, and may telephone the merchant with the results of the authenticity checker. Alternatively, or in addition, the communication link 64 may be over a network, including over the Internet, and the results of the authenticity checker 65 may be automatically sent to the merchant.

It is within the scope of embodiments of the present invention to provide in the manner described in connection with Fig. 6 a very large number of terminals dispersed over a geographically large region embracing one or more political subdivisions, countries, and even continents. The terminals may be located in pre-existing facilities of existing enterprises, such as banks, travel agencies, or insurance agencies. In this manner an individual may effectuate enrollment in accordance with Fig. 1 and later authenticate a transaction in the manner of Fig. 2 merely by going to a local terminal, with the result of the later authentication session being transmitted to the merchant via the communication link. As an alternative to using a terminal for authentication alone, it is equally possible to use a terminal to enter into the transaction simultaneously with the authentication process.

In Fig. 6, we have shown use, in connection with a single database 61, of two different types of physiological identifiers, fingerprint and utterance characteristics, one type of which (fingerprint) is more reliable than the other (utterance characteristics). On the other hand, the use of utterance for authentication may be accomplished over a telephone without the need for the user to go to a different physical location. It is within the scope of an embodiment of the present invention to store data pertaining to a plurality of physiological identifiers, and, with respect to a given transaction or circumstance, to select an identifier for authentication purposes that offers a desired trade-off between convenience and reliability. In other words, the use of a plurality of physiological identifiers permits adjustment of the reliability of the physiological identifier (by

selecting the appropriate type of identifier) to suit a desired level of reliability and therefore, for example, pricing. While Fig. 6 has illustrated fingerprint and utterance characteristics as the physiological identifiers utilized, other combinations may be utilized, for example, iris configuration and facial appearance.

The telephone may be used for providing an utterance for authentication in a manner previously described. In this context, although in Fig. 6 we have shown the physiological identifier transducer for utterances as a voice terminal/analyzer, in fact in related embodiments, the analyzer may be located remotely from the voice terminal. For example, the voice terminal may be as simple as a telephone in communication over a telephone line with a remotely located analyzer, and the analyzer may, for example, be physically adjacent to the database 61. In this manner may institute a telephone call to a central facility that includes the database 61, and the user's utterance may be analyzed with the resulting data run through an authenticity checker and the results provided to the merchant. In lieu of a telephone call to the central facility, the communication of the utterance may be over the Internet. Such an approach, while not as reliable as one that utilizes a human-monitored fingerprint reader, nevertheless provides a physiological identifier that lowers the risk of a fraudulent transaction. In other words, telephone authentication is well suited to circumstances where remote authentication is desired but physically distributed terminals of the type shown in Fig. 6 are not convenient.

An authentication system of the type described in various embodiments may be employed in a wide range of circumstances, including not only E-commerce but also, for example, distance learning and examination taking. In distance learning, the authentication system can be used to confirm actual attendance by persons purporting to be enrolled, and in examination taking, to confirm the authenticity of persons taking examinations. Thus, a system of the present type may be employed in any situation where a person is not physically present or is incapacitated, so normal in-person authentication is not possible or is difficult, and another party needs information about the person for the conduct

of some transaction or matter.

- The use of the various embodiments described above can reduce the risk of identity theft, because a merchant, intending to rely on the implicit representation that a subject is the one who the subject purports to be, now has
- 5 the benefit of a physiological identifier (as opposed to merely a password, etc., which may be stolen) confirming the subject's authenticity. Moreover, in a case where identity has already be stolen and a fraud perpetrated, a victim who has previously established a user data record in a multi-user personal information data base of the type described above may utilize the information in the user data
- 10 record to reestablish identity with one or more merchants. Indeed, an imposter who seeks to steal the identity of a user having a data record that is registered in the multi-user database, under circumstances where a reliable physiological identifier is employed to authenticate a transaction, must risk giving a fingerprint, for example, to the organization managing the multi-user database.
- 15 Because the imposter's fingerprint may then be accessed by law enforcement officials, for example, using normal warrant procedures, the chances of successful fraud are significantly reduced and a significant deterrent to fraud is also provided.

- Another context in which systems of the present type are applicable in
- 20 various embodiments is in connection with access to a user's medical information. Although access to a user's *personal information* (as defined above) is desirably restricted to merchants under controlled circumstances, access to at least some of a user's *medical information* (as defined above) (even when in the same database as the user's personal information) may be made more broadly
- 25 available to health care providers when a user is physically incapacitated. In this context it is convenient for the user to carry a card or other token to indicate that the user has provided medical information to the applicable multi-user database and even to identify in some manner (for example, by record number or a suitable alphanumeric identifier) the particular data record applicable to the
- 30 user's medical information. (Similarly, such an identifier may confirm to merchants that the user's personal information has been stored in the database,

as well as to facilitate look up of data in the data base.) A health care provider may then use information about the user to access pertinent medical information of the user. In this fashion, for example, the health care provider can have information permitting persons in a caring relationship to the user to be notified, and health care providers may be informed of information affecting treatment of the user. Current information about the status of the user's regular health care provider and health insurance may also be provided in this manner.

In implementing various embodiments described above, it is desirable for the manager of the database to prompt the user on a periodic basis, for example yearly, for an update of the user's personal information and medical information. When updated information is received, the data set of the user can be modified when appropriate authentication, as described, for example, in connection with Fig. 1, has been obtained from the user. It is a feature of embodiments of the present invention that the user's data set cannot be modified, for example, by a credit reporting agency, but only by the user on proper authentication. Given the inherent reliability of a database administered in this manner, it is within the scope of embodiments of the present invention to permit the database administrator on appropriate user authorization to provide change of address information, for example, to merchants.

Pursuant to a further embodiment of the present invention, the sponsor of a personal information data base of the type disclosed herein may provide a guarantee to a credit card issuer or other merchant that if the merchant first utilizes the sponsor's data base to authenticate the contact information or a change of address (offered by a purported user) before the merchant extends credit or effectuates a change of address, for example, then the liability of the merchant for a fraudulent transaction may be reduced or eliminated. In this way, the sponsor may provide a financial incentive to the merchant and justify charging the merchant for the opportunity to utilize the database.

It should be noted that various embodiments of the present invention do not require providing the merchant directly with personal data in the data base. Instead, for example, when a transaction is being authenticated, the merchant

need provide the data base sponsor only with a user's physiological identifier(s) (or a representation thereof) and a user's purported identity; the sponsor, upon checking the data base, can thereupon inform the merchant that, for the purported individual, there is a match between the physiological identifier(s) in
5 the data base and the physiological identifier(s) obtained by the merchant. The match determination may be carried out under control of the data base sponsor, or, alternatively, under control of the merchant.

- An institution such as a bank, in cooperation with the sponsor of a data base administered in accordance with various embodiments described above,
10 may offer a service, to protect a user, in which a user requires authentication, via use of the data base, of any check written over a certain amount. Indeed, such an approach may be utilized in connection not only with respect to a check but also with respect to any mechanism (credit or debit card transaction, electronic wallet transaction, digital money transaction, etc.) by which funds may be transferred.
- 15 The user may require authentication (via utilization of the data base) for any instance in which the funds to be transferred exceed a specified amount. In a related embodiment, the user may establish a list of exceptions to the authentication requirement, so that checks can be conveniently written to a spouse, etc.

What is claimed is:

1. A method of assuring integrity of a personal information data base containing personal information provided by multiple users, the method comprising:
 - 5 a. obtaining a user's personal information from the user;
 - b. obtaining a first set of physiological identifiers associated with the user;
 - c. storing, in a digital storage medium, a data set pertinent to the user, the data set including the user's personal information and a
 - 10 representation of the physiological identifiers associated with the user;
 - d. permitting a subject to modify information in the stored data set pertinent to the user only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a
 - 15 corresponding member of the first set, so that the subject is authenticated as the user.
2. A method according to claim 1, further comprising obtaining a user's medical information from the user, and wherein the data set includes the user's medical information.
- 20 3. A method according to claim 1, wherein the first set includes a plurality of members.
4. A method according to claim 1, wherein the first set of physiological identifiers includes the appearance of the user's face.
5. A method according to claim 1, wherein the first set of physiological
- 25 identifiers includes characteristics of utterances of the user.
6. A method according to claim 1, wherein the first set of physiological identifiers includes a fingerprint of the user.
7. A method according to claim 1, wherein the first set of physiological identifiers includes the configuration of an iris in an eye of the user.
- 30 8. A method according to claim 1, wherein the first set includes at least one member selected from the group consisting of a fingerprint of the user and an

the configuration of an iris in an eye of the user and at least one member selected from the group consisting of characteristics of utterances of the user and the appearance of the user's face.

9. A method according to claim 1, wherein, pursuant to step (d), a
5 subject is permitted to modify information in the stored data set only if the subject provides the new set of physiological identifiers under a condition permitting verification, independent of the physiological identifiers, that the new set is being provided by the person purporting to provide them.

- 10 10. A method according to claim 9, wherein the condition includes the physical presence of the subject when providing the new set.

11. A method according to claim 9, wherein the condition includes having the subject provide the new set when prompted to do so.

12. A method according to claim 9, wherein the condition includes having the subject provide a non-physiological identifier.

- 15 13. A method according to claim 12, wherein the non-physiological identifier is selected from the group consisting of a password and a pass card.

14. A method according to claim 9, wherein the non-physiological identifier is provided in the course of a session, over a computer network, employing a user's public and private keys.

- 20 15. A method according to claim 1, further comprising:
prompting a user, on a periodic basis, to update the data set pertinent to the user.

16. A method for authenticating a user transaction, the method comprising:

- 25 obtaining a test set of physiological identifiers from a subject purporting to be the user;

accessing information in the data set pertinent to the user stored in accordance with the method of claim 1; and

- 30 determining if there is a sufficient match between at least one member in the test set and a corresponding physiological identifier represented in the data set.

17. A method for authenticating a user transaction, the method comprising:

obtaining a test set of physiological identifiers from a subject purporting to be a specific user;

5 accessing information in a first data set pertinent to the specific user stored in a data base, the data base containing information provided by multiple users in a separate data set for each user, each data set including personal information of a user and a representation of a first set of physiological identifiers associated with the user, the data base being maintained under conditions wherein modification
10 by a subject of information in a stored data set pertinent to the subject is permitted only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as the user; and

15 determining if there is a sufficient match between at least one member in the test set and a corresponding physiological identifier represented in the data set.

18. A method according to claim 17, wherein:

the database is accessible via a server at a first location;

20 obtaining the test of physiological identifiers is performed at a second location remote from the first location;

determining if there is a sufficient match includes communicating with the server from the second location over a network.

19. A method according to claim 18, wherein:

25 obtaining the test set of physiological identifiers is performed under supervision of a merchant.

20. A method according to claim 19, wherein:

determining if there is a sufficient match is performed without revealing content of the first data set to the merchant.

30 21. A method according to any of claims 18 through 20, wherein the transaction is a change of address for an account.

22. A method according to any of claims 18 through 20, wherein the transaction is an application to open an account.
23. A method according to claim 21, wherein the account authorizes the transfer of funds.
- 5 24. A method according to claim 22, wherein the account authorizes the transfer of funds.
25. A method according to claim 21, wherein the account is based on the extension of credit to the account holder.
26. A method according to claim 22, wherein the account is based on the
10 extension of credit to the account holder.
27. A method according to claim 18, wherein the transaction is an application to a government agency for one of a license and a renewal of a license.
28. A method according to claim 18, wherein the transaction is an application to a government agency for one of an identification token and a
15 renewal of an identification token.
29. A digital storage medium on which has been recorded a multi-user personal information data base, the data base comprising, for each user, a data set pertinent to such user, the data set including:
- (a) such user's personal information obtained from the user;
- 20 (b) a representation of a first set of physiological identifiers associated with the user; and
- (c) such user's emergency information obtained from the user.
30. A system for updating a personal information database containing a data set for each one of multiple users, each data set including a user's personal
25 information and a representation of a first set of physiological identifiers associated with the user, the system comprising:
- a. a physiological identifier transducer having an output representing a physiological identifier associated with a subject;
- b. a user access authorization module, coupled to the
30 physiological identifier transducer, the database, for determining whether the output of the physiological identifier transducer sufficiently matches the

representation of the first set of physiological identifiers, so that the subject is authenticated as the user;

c. a user data set access module, coupled to the user access authorization module and to the database, for accessing the user data set, in the event that the user access authorization module has authenticated the subject as the user; and

d. a user data set update module, coupled to the database and to a user input, permitting the user to update such user's corresponding data set in the database.

- 10 31. A system for authenticating transactions, the system comprising:
- a. a multi-user personal information data base, the data base comprising, for each user, a data set pertinent to such user, the data set including:
 - i. such user's personal information obtained from the user;
 - 15 ii. a representation of a first set of physiological identifiers associated with the user;
 - b. a multiplicity of remotely distributed terminals in communication with the data base, each terminal including a physiological identifier transducer and a communication link with a merchant; and
 - 20 c. an authenticity checker, which determines whether there is a sufficient match between the output of a physiological identifier transducer attributable to a subject purporting to be a user and a physiological identifier in the first set.

25 32. A system according to claim 31, wherein the first set includes a plurality of members.

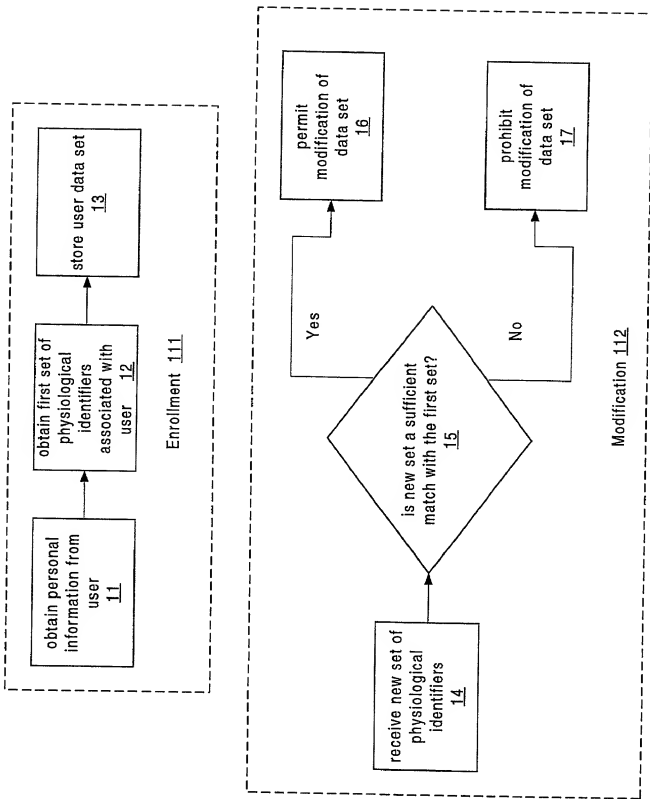
30 33. A system according to claim 31, wherein the first set includes at least one member selected from the group consisting of a fingerprint of the user and the configuration of an iris in an eye of the user and at least one member selected from the group consisting of characteristics of utterances of the user and the appearance of the user's face.

**Apparatus and Method for Authenticated Multi-User
Personal Information Database**

Abstract

- 5 A method of assuring integrity of a personal information in a data base containing personal information provided by multiple users uses in various embodiments physiological identifiers associated with each of the users. Related systems are also provided.

Fig. 1



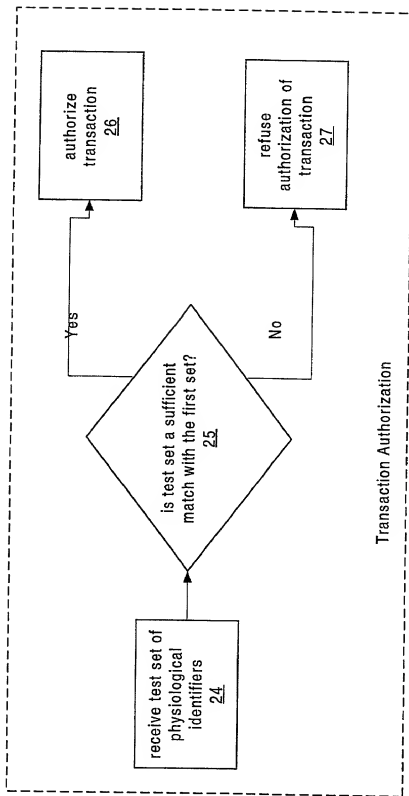
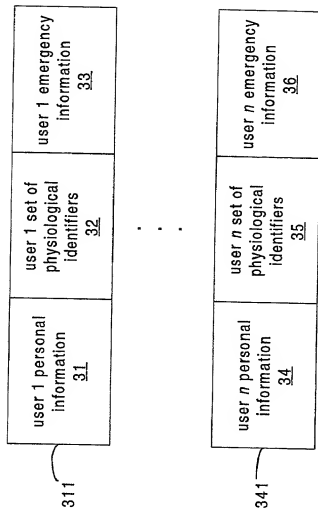


Fig. 2

Fig. 3



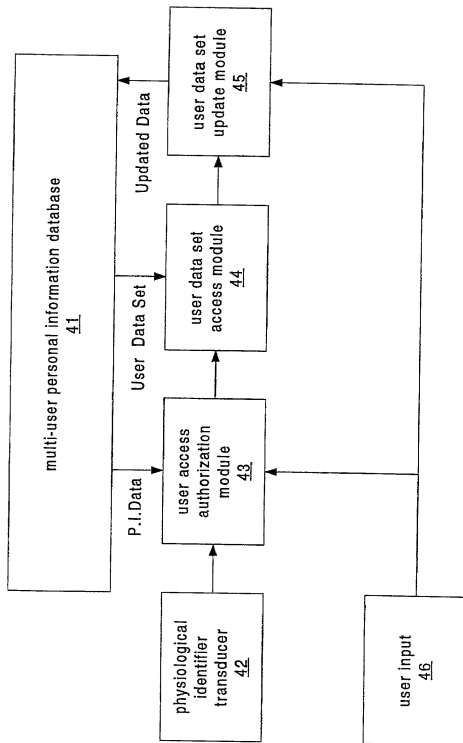


Fig. 4

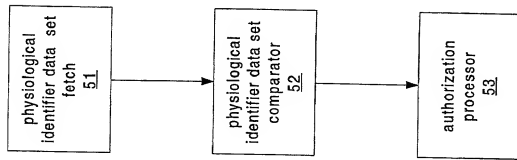


Fig. 5

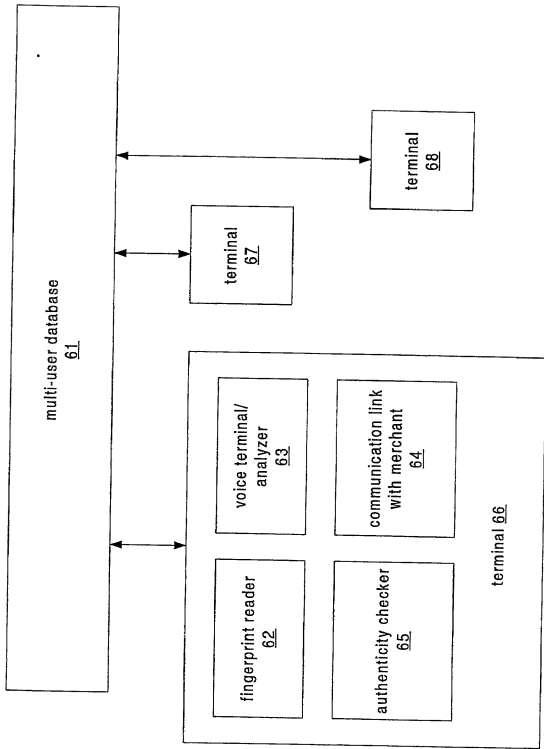


Fig. 6

Docket No.

2308/102

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

APPARATUS AND METHOD FOR AUTHENTICATED MULTI-USER PERSONAL INFORMATION DATABASE

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International Application Number _____ and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

(Application Serial No.)

(Filing Date)

(Application Serial No.)

(Filing Date)

(Application Serial No.)

(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Bruce D. Sunstein	Reg. No. 27,234	Elizabeth P. Morano	Reg. No. 42,904
Robert M. Asher	Reg. No. 30,445	Sonia K. Guterman	Reg. No. 44,729
Timothy M. Murphy	Reg. No. 33,198	Keith J. Wood	Reg. No. 45,235
Steven G. Saunders	Reg. No. 36,265	Karen A. Buchanan	Reg. No. 37,790
Harriet M. Strimpel	Reg. No. 37,008		
Samuel J. Petuchowski	Reg. No. 37,910		
Jeffrey T. Klayman	Reg. No. 39,250		
John J. Stickevers	Reg. No. 39,387		
Herbert A. Newborn	Reg. No. 42,031		
Jean M. Tibbetts	Reg. No. 43,193		
Jay Sandvos	Reg. No. 43,900		

Send Correspondence to: **Bruce D. Sunstein**
Bromberg & Sunstein LLP
 125 Summer Street Boston,
 Boston, MA 02110

Direct Telephone Calls to: *(name and telephone number)*
Bruce D. Sunstein (617) 443-9292

Full name of sole or first inventor Bruce D. Sunstein	
Sole or first inventor's signature	Date
Residence 20 Francis Street, Brookline, Massachusetts 02446	
Citizenship U.S.	
Post Office Address Same as residence	

Full name of second inventor, if any Eileen C. Shapiro	
Second inventor's signature	Date
Residence 987 Memorial Drive, Apt. 672, Cambridge, Massachusetts 02138	
Citizenship U.S.	
Post Office Address Same as residence	